REMARKS

This Amendment is submitted in response to the Office Action dated August 10, 2005, having a shortened statutory period set to expire November 10, 2005.

The present amendment proposes amending Claims 1, 3, 4, 7 and 18, cancelling Claims 27-29, and adding Claims 34-36. Upon entry of the proposed amendments, Claims 1-26 and 30-36 will be pending.

Rejections under 35 U.S.C. Section 102(e)

In paragraph 2 of the present Office Action, the Examiner has rejected Claims 1-33 under 35 U.S.C. § 102(e) as being anticipated by Morisawa et al. (U.S. Patent No. 5,537,544 – "*Morisawa*"). Applicants respectfully traverse these rejections.

With regards to exemplary Claim 1, the cited prior art does not teach or suggest authorizing a writing of data into a restricted portion of a computer's system memory "only by a trusted software entity...(that is) in a Basic Input/Output System (BIOS) Power-On Self Test (POST) program" (emphasis added), as supported in the present specification at, *inter alia*, page10, lines 16-17. *Morisawa* teaches that passwords can be stored in a "password memory means 1." However, password memory means 1 is distinct from BIOS, since a password from password memory means 1 enables the initial accessing of a BIOS flash memory (*Morisawa*, col. 6, lines 35-40). Furthermore, *Morisawa* never teaches or suggests a trusted software entity, which authorizes writing data (including passwords) into a restricted portion of the computer's system memory, being part of the POST program.

Furthermore, the cited art does not teach or suggest "copying security data from an unsecure memory device in a computer to a restricted portion of the computer's system memory...wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system." While *Morisawa* does teach "holding one or more registered passwords as being unreadable by direct access from the main processor section" and hiding "the password memory from the main processor section" by having a memory bus that is independent of the system bus (*Morisawa*, col. 3, lines 4-24), there is no teaching or suggestion in the prior art of storing security data into

"a restricted portion of the computer's system memory...(that) contains code and data needed for low level system control functions that are independent of the operating system," such as the SMI area (see Claims 30-33).

With regards to exemplary Claim 3, the cited prior art does not teach or suggest "checking a return address for a call requesting that the security data be copied to verify that the call originated with a trusted routine." *Morisawa* teaches (e.g., at col. 8, lines 15-55) unlocking different computer resources if a proper password is entered, but there is no mention of checking a return address of the trusted routine described in base Claim 1, in order to verify that the call originated with the trusted routine.

Exemplary Claim 4 claims detailed steps related to checking the return address, for the call that requested that security data be copied, to verify that the call originated with the trusted routine. These steps include placing an address for the BIOS code (which causes the security data to be copied to the restricted portion of system memory) in a label in BIOS ("placing an address for the label within code executing within the restricted portion of system memory"). The address for this label is sent along with the instructions for the call request ("placing a label...immediately after instructions for the call requesting that the security data be copied"). If the "return address for the call requesting that the security data be copied" does not match "the address for the label," then the security data is not copied into the restricted portion of system memory. *Morisawa*, and particularly at the cite passages by the Examiner in columns 10, 11 and 20, describes the general use of passwords, but does not teach or suggest the described claimed features including labels and addresses.

With regards to Claims 30-33, the cited art does not teach or suggest writing data for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory, wherein "the restricted portion of the system memory is a System Management Interrupt (SMI) memory space," as supported in the present specification at, *inter alia*, page 10, line 30 to page 11, line 1.

With regards to new Claim 34 (which is supported, *inter alia*, by Figure 2 and the associated written description on pages 9-11), the cited prior art does note teach or suggest "in response to a call to code in a System Memory Interrupt (SMI) memory space, using the code in

the SMI memory space to move the sensitive data from the non-protected system memory to the SMI memory space." Furthermore, the cited art does not teach or suggest moving the sensitive data from non-volatile memory to a non-secured system memory, and then from the non-secured system memory to SMI memory space as claimed.

With regards to new Claim 35 (which is supported, *inter alia*, by block 208 of Figure 2 and the associated written description), the cited prior art does not teach or suggest "wherein the move of sensitive data from the non-protected system to the SMI memory space is permitted only if the call is a first request to copy the sensitive data from the non-protected system memory to the SMI memory space" (emphasis added).

With regards to new Claim 36 (which is supported, *inter alia*, by Figure 2 and the associated written description on pages 9-10), the cited prior art does not teach or suggest "appending a label to a source code in the BIOS POST program, wherein the source code calls the code in the SMI memory space, and wherein the label contains an address of the source code; checking on a stack a return address for the source code when the source code calls the code in the SMI memory space; comparing the return address on the stack with the address in the label for the source code; and storing the sensitive data from the non-protected system memory to the SMI memory space only in response to determining that the address on the stack is the same as the address in the label for the source code." As stated above, *Morisawa* does not teach or suggest the use of addresses to confirm whether code, which calls other code in the SMI memory space to move sensitive data from non-protected system memory to SMI memory space, is trustworthy ("only in response to determining...").

CONCLUSION

As the cited art does not teach or suggest all of the limitations presently claimed, Applicants respectfully request a Notice of Allowance for all pending claims.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563.**

Respectfully submitted,

James E. Boice
Registration No. 44,545
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)